PDR RID Report

Originator	Arthur S. Gaylord	**Phone No**	413-545-2520	**RID ID PDR** 135
Organization	University or Massachusetts			**Review** CSMS
E Mail Address	art@cs.umass.edu			**Originator Ref**
Document	CSMS PDR - ISS			**Priority** 1

Section **Page** **Figure Table**

Category Name System-level **Actionee** HAIS

Sub Category RMA

Subject EOC LAN reliability

Description of Problem or Suggestion:

The analysis of the EOC LAN mean downtime is based solely on hardware failures. Software and system failures should also be considered to insure that the requirements for availability and MDT are met for the overall EOC LAN. Differences in the operation and support LANs will make it difficult to test and resolve failures in the support LAN environment. In particular there is a concern of how system and middle level software will respond in intermittent network failures.

NASA reliability standards assume that software doesn't fail, because it is assumed it passes NASA QA standards during development. This is not true for COTS software, even that embedded in products!

Originator's Recommendation

Expand failure /reliability analysis to include software failures, at least to the extent that failovers to replicated servers can be guaranteed to occur within required time intervals.
The support LAN should have greater hardware compatibility with the operational LAN. At least a couple of servers should bee dual-attached within the support LAN.

GSFC Response by: **GSFC Response Date**

HAIS Response by: Forman **HAIS Schedule** 2/10/95

HAIS R. E. Armstrong **HAIS Response Date** 2/10/95

This RID raises two issues: (1) whether hosts should be dual-homed to the EOC support LAN in order to be able to completely simulate failures on the operational LAN; and (2) whether software reliability should be considered in overall reliability and availability estimates.

Regarding (1), the fail-over scenario for EOC hosts dual-attached to the Operational LAN is totally transparent to application-layer software (and even to transport and network layer software such as TCP/IP). The fail-over capability will be tested as part of the activation and turnover of the EOC network hardware (e.g., by powering off a hub and verifying that all FDDI hosts continue to have full connectivity). This type of test is generally performed only at installation or after major network configuration changes. If desired, FOS can perform such tests without the need to dual-attach hosts to the Support LAN. FOS can simply interchange the dual-attached interface with the single-attached interface so that the Support LAN interface is dual-attached to the Support LAN hubs. Because the failure scenario and recovery are transparent to application software, the test could also be performed with any free workstation(s) by dual-attaching it to spare ports on the Support LAN hubs. For this reason, and because dual-attaching Support LAN hosts adds cost and complexity to the design, FOS and CSMS do not believe that dual-attachments are necessary for software failure testing.

Regarding (2), it is not feasible to perform software reliability predictions on a COTS environment system due to the unavailibility of software Mean-Time-Between-Failures (MTBF) and Mean-Down-Time(MDT) data from COTS vendors. However, during the operational phase of the ECS, the required operational availability (Ao) and mean-down-time (MDT) will be assessed by analyzing actual software and hardware discrepancies of the ECS subsystems.

Status **Closed** **Date Closed** **3/8/95** **Sponsor** **desJardins**

****** **Attachment if any** ******

****** Attachment if any ******